UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/676,474	09/30/2003	Klimenty Vainstein	2222.5450000	7534

26111 7590 04/13/2010

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
PALIWAL, YOGESH	
ART UNIT	PAPER NUMBER
2435	
MAIL DATE	DELIVERY MODE
04/13/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/676,474	VAINSTEIN ET AL.	
	Examiner	Art Unit	
	YOGESH PALIWAL	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 January 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- Applicant's amendment filed on 1/8/2010 has been entered. Applicant has amended claims 1, 2, 4, 9, 11-14, 19, 21, 22, 27, and 28. Currently claims 1-28 are pending in this application.

Response to Arguments

Applicant's arguments filed 1/8/2010 have been fully considered but they are not persuasive for following reasons:

Independent Claim 1, 14, and 27

- Applicant argues that, "Serbinis does not disclose that "transition rules specify circumstances under which a secured document is to transition from one state to another, and wherein the circumstances include the occurrence and internal and external events," as recited in claim 1. Serbinis also fails to disclose "receiving an event, wherein the event is one of a group of internal and external events" as recited, using respective language, in claims 14 and 27. Anticipation under 35 U.S.C. § 102 requires showing the presence in a single.
- Examiner respectfully disagrees and maintains that Serbinis explicitly discloses transition rules specify circumstances under which a secured document is to transition from one state to another (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active.") and wherein the circumstances include the occurrence of internal and external events

(see, Column 7, lines 63- 67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time." And also Column 8, lines 26-29, "Document instances are marked "canceled" when an Authorized User (typically the Originator) forces a document to expire before the expiration time"). Note: Applicant defines (see, paragraph 0051 of PGPub) "Typically, the transition rules are triggered by the occurrence of events. The events can be internal or external. The external events can originate from users or from another system (e.g., a document management system)". Since applicant has defined that external events originate from users of from another system, examiner is equating an authorized user forcing document to expire before the expiration date to an external event. Since changing of state based on active date/time occurs automatically without user's interference examiner is interpreting it as an internal event.

- Applicant further argues that, "Serbinis further discloses that "according to the authorization information *submitted by a document originator,* new document rights, document group rights and document instance rights are created for the document" in the DMS system and that "the Authorized User is a *pre-registered* Authorized *User* with *trusted credentials"* (Serbinis, col. 7, lines 57-64 and col. 13, lines 13-14). Applicants submit when such "Authorized Users" and "document originators" forces a document to expire, this is an internal event within Serbinis'

DMS system. Nowhere does Serbinis disclose "receiving an event, wherein the event is one of a group of internal and external events" as recited, using respective language, in claims 14 and 27.

- Examiner is puzzled with the above remark because applicant admitted that "such "Authorized Users" and "document originators" forces a document to expire, this is an internal event within Serbinis' DMS system" and then further recites that "Nowhere does Serbinis disclose "receiving an event, wherein the event is one of a group of internal and external events". It seems like applicant agrees that Serbinis discloses internal event (Note: In view of specification, examiner is interpreting this event as external event) but then allege that Serbinis does not disclose receiving an event, wherein the event is **one of a group** of internal and external events.
- Applicant further argues that, "Further, as discussed during the aforementioned telephonic interview, in Serbinis' system "[s]tates for a document instance" are limited to ""pending," "active," "archived," "canceled" and "deleted"" (Serbinis, col. 7, line 67 - col. 8, line 1). In contrast to the above-noted distinguishing features of claims 1, 14, and 27, Serbinis describes that "[c]anceled document instances then are treated like archived document instances" (Serbinis, col. 8, lines 26-31). Thus, Serbinis fails to teach or suggest at least wherein each of the *different states* is associated with one or more access restrictions, and wherein *each of the different states has distinct access restrictions for secured documents which reside in that state,* as recited, using respective language, in

claims 1,14, and 27. Even assuming for the sake of argument that the Examiner's interpretation of Serbinis' states for a document instance is correct (which Applicants disagree with), Serbinis, in the sections cited by the Examiner, or in other sections, contains no disclosure of the above-quoted distinct access restriction features of claims 1, 14, and 27. As discussed during the aforementioned interview, Applicants submit that Serbinis' document instance states are not analogous to a "process-driven security policy" which Claims 12, 19 and 20 were rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Serbinis in view of U.S. Patent No. 6,341,164 to Dilkie *et al.* ("Dilkie").

- Examiner once again disagrees and would like to point out that Serbinis explicitly discloses wherein each of the *different states* is associated with one or more access restrictions, and wherein *each of the different states has distinct access restrictions for secured documents which reside in that state* (see, Column 8, lines 1-20, "A "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all Authorized Users."). Note examiner is interpreting only the pending and active states to the plurality of different states. Further note that examiner has already addressed applicant's argument regarding canceled document instances then are treated like archived document instances and further point out that examiner is only interpreting active and pending states to the plurality of different states therefore the fact that canceled and archived have identical access restriction ir not

relevant in view of the examiner's interpretation of plurality of different states which only include active and pending states.

Dependent Claim 9

Applicant's arguments with respect to claim 9 have been considered but are moot in view of the new ground(s) of rejection.

Dependent Claim 13

- Applicant argues that, "Moreover, claim 13 as amended herein recites, "in response to determining, by the access manager, that access to a secured document is permitted by a requestor, access to the secured document is available at a client machine associated with the requestor." Applicants submit that Serbinis also fails to disclose this feature. For this additional reason, claim 13 should be found allowable over the applied reference."
- Examiner respectfully disagrees and would like to point out that Serbinis explicitly discloses in response to determining, by the access manager, that access to a secured document is permitted by a requestor, access to the secured document is available at a client machine associated with the requestor (see, Column 9 line 66- Column 10, line 5, "The Authorized User may then request retrieval of the document from store 30, at step 88, and any automatic filtering, or filtering selected by the Authorized User, may be performed during the document download process at step 89. The document is then downloaded to the

Authorized User at step 90. Each transaction is logged to the appropriate tables of DMS database 25.")

Note: Applicant relied upon similar argument for other independent and dependent claim rejection. Arguments discussed above are not found persuasive. As a result rejection of all other independent claims and dependent claims are also maintained for the same rational.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 22 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Currently claim 22 recites "wherein the external events are external to the server computer and the client computer". Paragraph 0073 (PGpub) of the applicants' specification recites "external events can originate from users or from another system (e.g., a document management system)." There is no explicit support for the language requiring "external events are external to the server computer and the client computer".

Correction/Classification is required.

Claim Objections

Claims1-13 and 28 are objected to because of the following informalities: In claims 1 and 28, "wherein the circumstance include the occurrence and internal and external events", should read, "wherein the circumstance include the occurrence of internal and external events". Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-8, 11, 13-18 and 27 are rejected under 35 U.S.C. 102(e) as being anticipated by Serbinis et al. (US 6,584,466 B1), hereinafter "Serbinis".

Regarding **Claim 1**, Serbinis discloses a document security system for restricting access to secured documents (See Fig. 1-5) comprising:

a processor (see, Fig. 1B, numerals 20 A, 20 B);

a policy module configured to enable the processor to store at least one process-driven security policy (see, Column 7, lines 63-67, "document state process") on a computer readable storage medium, wherein the process-driven security policy includes a plurality of different states (see, Column 7 line 67- Column 8, line 4, "pending," and "active," states. Note: examiner is equating only pending and active to the claimed plurality of different states) and transition rules (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active.""), wherein each of the different states is associated with one or more access restrictions, and wherein each of the different states has distinct access restrictions for secured documents which reside in that state (see, Column 8, lines 1-20, "A "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all Authorized Users.") and wherein the transition rules specify circumstances under which a secured document is to transition from one state to another (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active.") and wherein the circumstances include the occurrence of internal and external events (see, Column 7, lines 63- 67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time." And also Column 8, lines

26-29, "Document instances are marked "canceled" when an Authorized User (typically the Originator) forces a document to expire before the expiration time"). Note: see reply to arguments section for detailed explanation).

an access manager module configured to enable the processor to access the process-driven security policy and determine whether access to a secured document is permitted by a requestor based on the policy state associated therewith at the time access is requested and the corresponding one or more access restrictions thereof for the process-driven security policy (see, Column 9, line 64- Column 10 line 5 and also Column 8, lines 1-20, Column 9, line 64- Column 10 line 5 describing the authentication process and Column 8, lines 1-20, discloses a "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all Authorized Users, so the authentication step determine the access based on policy state associated therewith at the time access is requested and the corresponding one or more access restriction thereof for the process-driven security policy).

Regarding **Claim 2,** the rejection of claim 1 is incorporated and Serbinis further discloses that the one or more access restrictions for the secured document are automatically changed in response to detecting a change in the state of the process-driven security policy for the secured document (see Column 7, lines 63-67).

Regarding **Claim 3,** the rejection of claim 1 is incorporated and Serbinis further discloses that events cause the state of the process-driven security policy for the secured document to automatically transition from one state to another (see, Column 7, lines 63-67).

Regarding **Claim 4**, the rejection of claim 3 is incorporated and Serbinis further discloses wherein the internal events originate from the document security system and wherein external events originate from outside the document security system (see, Column 7, lines 63- 67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time." And also Column 8, lines 26-29, "Document instances are marked "canceled" when an Authorized User (typically the Originator) forces a document to expire before the expiration time").

Regarding **Claim 5**, the rejection of claim 4 is incorporated and Serbinis further discloses that at least one of the events is an external event from a document management system (see Column 8, lines 26-30).

Regarding **Claim 6**, the rejection of claim 1 is incorporated and Serbinis further discloses that one or more of the corresponding one or more access restrictions for access to the secured document remain intact when the state of the process-driven security policy for the secured document changes (see paragraph 0123)

Regarding **Claim 7**, the rejection of claim 1 is incorporated and Serbinis further discloses that events cause the state of the process-driven security policy to automatically transition from one state to another (see Column 7, lines 63-67).

wherein the process-driven security policy includes at least a first state and a second state, and wherein a first event causes transition from the first state to the

second state and a third state and second event that causes transition from the second state to a third state (see, Column 8, lines 1-20).

Regarding **Claim 8**, the rejection of claim 1 is incorporated and Serbinis further discloses that events cause the state of the process-driven security policy to automatically transition from one state to another (see Column 7, lines 63-67).

wherein the process-driven security policy includes at least a first state and a second state, and wherein a first event causes transition from the first state to the second state (see Column 8, lines 1-20).

Regarding **Claim 11**, the rejection of claim 1 is incorporated and Serbinis further discloses that events cause the state of the process-driven security policy for the secured document to transition from a previous state to a current state, and wherein the secured document is modified in response to detecting a transition from the previous state of the process-driven security policy for the secured document (see Column 7, lines 63-67).

Regarding **Claim 13**, the rejection of claim 11 is incorporated and Serbinis further discloses wherein in response to determining, by the access manager, that access to a secured document is permitted by a requestor, access to the secured document is available at a client machine associated with the requestor (see, Column 9 line 66-Column 10, line 5, "The Authorized User may then request retrieval of the document from store 30, at step 88, and any automatic filtering, or filtering selected by the Authorized User, may be performed during the document download process at step 89.

The document is then downloaded to the Authorized User at step 90. Each transaction is logged to the appropriate tables of DMS database 25.").

Regarding **Claims 14 and 27**, Serbinis discloses a method and a corresponding software program for transitioning at least one secured document through a security-policy state machine having a plurality of different states (see, Column 7 line 67-Column 8, line 4, "pending," and "active," states, Note: examiner is equating only pending and active states to the claimed plurality of different states), each of the plurality of different states having distinct access restrictions for secured documents which reside in that state (see, Column 8, lines 1-20, "A "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all Authorized Users."), the method comprising:

receiving an event (see, Column 7, lines 63-67, "the active date/time, and expiration date/time"), wherein the event is one of a group on internal and external events (see, Column 7, lines 63- 67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time." And also Column 8, lines 26-29, "Document instances are marked "canceled" when an Authorized User (typically the Originator) forces a document to expire before the expiration time"). Note: see reply to arguments section for detailed explanation).

determining whether the event causes a state transition for the at least one secured document from a former state to a subsequent different state of the security-

policy state machine; (see, Column 7, lines 63-67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process")

automatically transitioning from the former state to the subsequent different state of the security-policy state machine in response to determining that the event causes the state transition (see, Column 7, lines 63-67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time.")

Regarding **Claim 15**, the rejection of claim 14 is incorporated and Serbinis further discloses the security-policy state machine implements a process-driven security policy, and wherein each state of the security-policy state machine has different access restrictions (see Column 8, lines 1-20).

Regarding **Claim 16**, the rejection of claim 14 is incorporated and Serbinis further discloses each of the states of the security-policy state machine have different access policies (see Column 8, lines 1-20).

Regarding **Claim 17**, the rejection of claim 16 is incorporated and Serbinis further discloses the security-policy state machine is provided as part of a document security system, and wherein the different access policies of the security-policy state machine are enforced by the document security system (See, Column 8, lines 1-20 and Column 9, line 63- Column 10, line 5)

Regarding **Claim 18,** the rejection of claim 14 is incorporated and Serbinis further discloses wherein the transitioning comprises modifying the secured document to reflect the subsequent state of the security-policy state machine (see Column 7, lines 63-67).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Serbinis in view of Dutta et al. (US 6976259 B1), hereinafter, "Dutta".

Regarding **Claim 9,** the rejection of claim 1 is incorporated and Serbinis does not explicitly disclose wherein the external events originate from a second document security system.

Dutta et al. (US 6,976,259 B1) discloses document security system (see, Fig. 2, Numeral 70) in which change to states is triggered by external events which are originated from a second document security system (see, Fig. 2 and also Column 6, lines 17-23).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to add, in the system of Serbinis, a server which administer state changes for the document security system as taught by Dutta because "In this

way, the system is more flexible in that changes made in a central location (e.g. object store 70) are replicated to a plurality of clients." (Dutta, Column 6, lines 21-23).

Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Serbinis in view of Li et al. (US 2004/0193912 A1), hereinafter Li.

Regarding **Claim 10**, the rejection of claim 9 is incorporated and Serbinis does not teach that the transition rules are written in XML.

However, Smith et al. in the same field of endeavor of network security discloses writing security policies in XML format (Paragraph 0014, "In one embodiment of the present invention, the security policies are stored in a relational database in a native Extensible Markup Language (XML) format")

Therefor, it would have been obvious at the time the invention was made to one of ordinary skill in the art to write the transition rules of Serbinis in XML format as taught by Li because XML is a text-based and platform independent, as a result policy server would be able to enforce and distribute the policies to all client having any type of operating system platform.

Claims 12, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Serbinis in view of Dilkie et al. (US 6341164), hereinafter "Dilkie".

Regarding **Claim 12**, the rejection of claim 11 is incorporated and Serbinis further discloses that the secured document includes at least a security information portion (see, Column 9, lines 21-25 and Column 7, lines 33-40) and an encrypted data portion

(see, Column 11, lines 7-10) and further discloses transitioning secure document from the previous state to the current state (see, Column 7, lines 63-67).

Serbinis discloses encrypting document with the session key and require the retriever of the document to provide the same key to decrypt the documents. However, Serbinis does not explicitly discloses the security information portion including at least an encrypted key, and the key being encrypted is decrypted in order to decrypt the encrypted data portion and wherein if the process-driven security policy for the secured document transitions from the previous state to the current state, the secured document is modified by decrypting the encrypted key and then re-encrypting the key, whereby the key is encrypted differently for the current state than the previous state.

However, Dilkie discloses security information portion including at least an encrypted key (Column 4 lines 1-3, "A cryptographic key package may include, for example, a symmetric encryption key wrapped, or encrypted, with an asymmetric encryption key, such as a recipient's public key..."), and the key being encrypted is decrypted in order to decrypt the encrypted data portion (Column 7 lines 46-50, "The corresponding private key (for example, signing key) is used to unwrap the cryptographic key package to recover a message encryption key as known in the art. The system may re-encrypt the key package with a different asymmetric key and/or algorithm as shown in block 409. The analyzer 103 may then decrypt the message data in any suitable manner using the message encryption key as shown in block 410".) and wherein when, the secured document is modified by decrypting the encrypted key and then re-encrypting the key, whereby the key is encrypted differently for the modified

document (Column 7 lines 46-50, "The corresponding private key (for example, signing key) is used to unwrap the cryptographic key package to recover a message encryption key as known in the art. The system may re-encrypt the key package with a different asymmetric key and/or algorithm as shown in block 409. The analyzer 103 may then decrypt the message data in any suitable manner using the message encryption key as shown in block 410".).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to improve the encryption system of Serbinis by encrypting the session key using the public key as taught by Dikkie because it provides extra security and provide secure session key exchange. It would have been further obvious to modify the secured document of Serbinis by decrypting the encrypted key and then re-encrypting the key as taught by Dilkie when document transit from one state to another state as taught by Serbinis so that system would need to re-encrypt the "header without re-encrypting the file itself, thereby only changing the wrapping on the header key" (Dilkie, column 8, lines 19-21)

Regarding **Claim 19**, the rejection of claim 14 is incorporated and Serbinis does not teach retrieving an encrypted file key from the secured document; decrypting the encrypted file key to yield a file key; subsequently encrypting the file key in accordance with the subsequent state of the security-policy state machine; and storing the secured document, the secured document including at least an encrypted data portion and the subsequently encrypted file key.

However, Dilkie discloses a method of retrieving an encrypted file key from the secured document; decrypting, the encrypted file key to yield a file key; subsequently encrypting the file key and storing the secured document, (column 8, lines 11-18, "incoming message is encrypted under algorithm X with symmetric key Y wrapped (encrypted) with asymmetric key Z, the system may decrypt asymmetrically to recover the symmetric key Y, and re-encrypt the symmetric key Y with a different asymmetric key Z' and replace the previous cryptographic key package with the new re-encrypted key data forming a new cryptographic key package in the header. The message data with the new cryptographic key package may then be stored") the secured document including at least an encrypted data portion (column 4, lines 7-8, "the encrypted message data with the header data") and the subsequently encrypted file key (Column 3, lines 62-63, "The cryptographic key package information is preferably contained as header data")

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the secured document by decrypting the encrypted key and then re-encrypting the key as taught by Dilkie when document transit from one state to another state as taught by Serbinis to re-encrypt the "*header without re-encrypting the file itself, thereby only changing the wrapping on the header key*" (Dilkie, column 8, lines 19-21)

Regarding **Claim 20**, the rejection of claim 14 is incorporated and Serbinis does not teach a method of retrieving an encrypted file key from the secured document; obtaining a private state key associated with the former state of the security-policy state

machine; decrypting the encrypted file key using the private file key; obtaining a public state key associated with the subsequent state of the security-policy state machine; subsequently encrypting the file key in accordance with the public state key; and storing the secured document, the secured document including at least an encrypted data portion and the subsequently encrypted file key.

However, Dilkie discloses a method of retrieving an encrypted file key from the secured document; obtaining a private state key associated with the former state of the security-policy state machine; decrypting the encrypted file key using the private file key; obtaining a public state key associated with the subsequent state of the security-policy state machine; subsequently encrypting the file key in accordance with the public state key; and storing the secured document, (column 8, lines 11-18, "incoming message is encrypted under algorithm X with symmetric key Y wrapped (encrypted) with asymmetric key Z, the system may decrypt asymmetrically to recover the symmetric key Y, and re-encrypt the symmetric key Y with a different asymmetric key Z' and replace the previous cryptographic key package with the new re-encrypted key data forming a new cryptographic key package in the header. The message data with the new cryptographic key package may then be stored") the secured document including at least an encrypted data portion (column 4, lines 7-8, "the encrypted message data with the header data") and the subsequently encrypted file key (Column 3, lines 62-63, "The cryptographic key package information is preferably contained as header data")

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the secured document by decrypting the encrypted

key and then re-encrypting the key as taught by Dilkie when document transit from one state to another state as taught by Serbinis to re-encrypt the *"header without re-encrypting the file itself, thereby only changing the wrapping on the header key"* (column 8, lines 19-21)

Claims 21, 23-26 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Serbinis in view of Leser et al. (US 2005/0028006 A1), hereinafter "Leser".

Regarding **Claim 21**, Serbinis discloses a method and corresponding computer program for imposing access restrictions on electronic documents, the method comprising:

providing at least one process-driven security policy at a server computer, wherein the process-driven security policy is associated with a plurality of different states (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active."") and wherein each of the different states has distinct access restriction for secured documents which reside in that state (see, Column 8, lines 1-20, "A "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all Authorized Users.");

Serbinis does not disclose: providing a reference to the process-driven security policy to client computer, the reference referring to the process-driven security policy resident on the server computer and associating the reference to an electronic document.

Leser discloses providing a reference to the process-driven security policy to client computer, the reference referring to the process-driven security policy resident on the server computer and associating the reference to an electronic document (see, Paragraph 0208, Note: Paragraph 0208 is fully supported by the provisional application at least at Page 32, lines 3-10).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to cache security-policy of the system of Serbinis into the user's computers thereby enabling them to generate and or use protected document while they are off-line.

The combination of Serbinis and Leser further discloses

transitioning the process-driven security policy from one state to a current state (see, Column 8, lines 1-20) in response to the occurrence of an event, wherein the event is one of group of internal and external events (see, Column 7, lines 63- 67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time." And also Column 8, lines 26-29, "Document instances are marked "canceled" when an Authorized User (typically the Originator) forces a document to expire before the expiration time"). Note: see reply to arguments section for detailed explanation); and

subsequently determining at the server computer whether a requestor is permitted to access the electronic document, the access being based on a current state of the process-driven security policy (see, Column 9, line 64- Column 10 line 5 and also

Column 8, lines 1-20), the current state being informed to the server computer by sending the reference to the server computer (see, Leser, Paragraph 0029, Note: Paragraph 0029 is fully supported by the provisional application at least at Page 9, lines 1-4).

Regarding **Claim 23**, the rejection of claim 22 is incorporated and Serbinis further discloses wherein the transitioning is performed at the server computer (see, Column 7, lines 63-67).

Regarding **Claim 24**, the rejection of claim 21 is incorporated and Serbinis further discloses wherein the associating associates the reference to a group of documents (See, Column 7, lines 22-23 as modified with Leser).

Regarding **Claim 25**, the rejection of claim 21 is incorporated and Serbinis further discloses wherein the method pertains to a group of electronic documents, and wherein all of the electronic documents of the group are always in the same state of the process-driven security policy (See Column 7, lines 54-57, Column 10, lines 59-64 and also Column 3, lines 16-27).

Regarding **Claim 26**, the rejection of claim 21 is incorporated and Serbinis further discloses evaluating the process-driven security policy of an electronic document at the server computer based on at least the security policy restrictions for the current state of the process-driven security policy for the electronic document (see Column 7, lines 63-67).

Regarding **Claim 28**, Serbinis discloses a computer program for imposing access restrictions on electronic documents, the program instructions comprising:

Instructions to providing at least one process-driven security policy at a server computer, wherein the process-driven security policy is associated with a plurality of different states (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active."") and transition rules associated therewith (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active."") and wherein each of the different states has distinct access restrictions for secured documents which reside in that state (see, Column 8, lines 1-20, "A "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all Authorized Users.") and wherein the transition rules specify circumstances under which a secured document is to transition from one state to another (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active.") and wherein the circumstances include the occurrence of internal and external events (see, Column 7, lines 63- 67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time." And also Column 8, lines 26-29, "Document instances are marked "canceled" when an Authorized User (typically the Originator) forces a document to expire before the expiration time"). Note: see reply to arguments section for detailed explanation).

Serbinis does not disclose: providing a reference to the process-driven security policy to client computer, the reference referring to the process-driven security policy resident on the server computer and associating the reference to an electronic document.

Leser discloses providing a reference to the process-driven security policy to client computer, the reference referring to the process-driven security policy resident on the server computer and associating the reference to an electronic document (see, Paragraph 0208, Note: Paragraph 0208 is fully supported by the provisional application at least at Page 32, lines 3-10).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to cache security-policy of the system of Serbinis into the user's computers thereby enabling them to generate and or use protected document while they are off-line.

The combination of Serbinis and Leser further discloses

transitioning the process-driven security policy from one state to a current state (see, Column 8, lines 1-20).

subsequently determining at the server computer whether a requestor is permitted to access the electronic document, the access being based on a current state of the process-driven security policy (see, Column 9, line 64- Column 10 line 5 and also Column 8, lines 1-20), the current state being informed to the server computer by sending the reference to the server computer (see, Leser, Paragraph 0029, Note:

Paragraph 0029 is fully supported by the provisional application at least at Page 9, lines 1-4).

Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Serbinis in view of Leser and further in view of Dutta.

Regarding **Claim 22**, the rejection of claim 21 is incorporated and the combination of Serbinis and Leser does not explicitly disclose wherein the external events are external to the server computer and the client computer.

However, Dutta discloses wherein external events are external to a document security server and the client computer (see, Fig. 2 and also Column 6, lines 17-23).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to add, in the system of Serbinis, a server which administer state changes for the document security system as taught by Dutta because "In this way, the system is more flexible in that changes made in a central location (e.g. object store 70) are replicated to a plurality of clients." (Dutta, Column 6, lines 21-23).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F 9:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 5712723859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435